UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/686,956	10/15/2003	Mitch Fredrick Singer	113748-4837US	8803

27189 7590 02/05/2010

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
530 B STREET
SUITE 2100
SAN DIEGO, CA 92101

EXAMINER	
DUNN, DARRIN D	

ART UNIT	PAPER NUMBER
2121	

NOTIFICATION DATE	DELIVERY MODE
02/05/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@procopio.com
PTONotifications@procopio.com

Office Action Summary	Application No.	Applicant(s)	
	10/686,956	SINGER ET AL.	
	Examiner	Art Unit	
	DARRIN DUNN	2121	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 November 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3 and 5-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3 and 5-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/29/09, 10/21/09, 08/27/09*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application.
6) ☐ Other: _____.

DETAILED ACTION

1. The Office Action is responsive to the communication filed on 11/20/2009.

2. Claims 1-3 and 5-39 are pending.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/20/2009 has been entered.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

6. Claims 1-3 and 5-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Messerges et al. (USPN 20020157002) in view over Foster et al. (USPN 20030198351) and in further view over Ikeda et al. (USPN 20060098936)

7. As per claim 1, Messerges et al. teaches a method of presenting content data, comprising:

receiving at a server device ([0042], [0054] e.g., domain authority, content provider, or other entity) a present request indicating locked content data ([0042] e.g., content package) from a client ([0050] e.g. user device) connected to a hub network ([Figure 2]);

checking a license corresponding to said locked content data to determine if said license permits said client to present said locked content data ([0049], [0060-61] e.g., verifying the package's rights document , hash, and encoded rights table),

wherein said locked content data is a bound instance if said license permits presentation of said locked content data by said client connected to the hub network ([0060-63], [0037- 38], [0040], [Figure 4] e.g., all devices registered to a domain will be interconnected in that they will have access to content within the domain. Content is cryptographically bound to the domain ID), and

wherein the bound instance of said locked content data and the license corresponding to said locked content data are bound to the hub network ([0060-63], [0037-38], [0040], e.g., content is bound to the device domain); and

presenting said locked content data through a presentation component connected to said client when said locked content data is a bound instance (([0059-63], [Figure 3] e.g, before

content may be played, the content manager invokes the core digital rights management software)

However, Messerges et al. does not teach the following limitations:

1] wherein the server device is configured to set up the hub network including adding the client and the server device to the hub network.

2] wherein the server device is configured to function as a client in the hub network, and

3] wherein said locked content data is stored on the server device connected to the hub network

Foster et al. teaches **1]** ([0080 lines 1-10] e.g., existing devices are both servers and authorizers. Authorizers are configured to authorize the addition of the new device.)

2] ([0080 line 9-11] e.g., sharing and distributing data, i.e., server may render content in the same manner as the client because devices are both authorizers and servers. It is understood that a participating device may render content. Since a device may be a server, it is understood that a server acts as a client (e.g., another device) because its is operable to play content in the same way as another device. It is interpreted that sharing a common function between a server and client enables a server to act as a client)

3] ([0078], [0080] lines 9-11] e.g., content is freely shared among devices, wherein a device may be a server and authorizer)

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to modify Messerges as to enable participating devices to function as a server and client, control how many devices are added to the network, and control how content is distributed within the network. The motivation is to implement the teachings of Foster et al. to localize content distribution opposed to requiring a client device to contact an external source for

content, as per Messerges. Thus, it is obvious to make integral (e.g., adding, distributing, and authorizing content) content distribution with that of a local network).

However, Messerges et al., as modified, does not teach a) wherein said locked content data is changed to a discrete instance when said locked content data is to be moved to another server device bound to another hub network and b) the server device sends a disable request for the locked content data to clients of the hub network to indicate that the bound instance of the locked content data is changed to the discrete instance. Messerges et al. does teach the limitation of when said locked content data is to be moved to another server device bound to another hub network (see Fosters, [0079] e.g., obvious to relocate content to another domain. However, the copy will be disabled, see below, until rights are established via a source for that copy. As applied, a copy would be operable to be bound to another network by requesting such content to be bound, as per the teachings of Messerges, [0037] e.g., binding content to a particular domain);

Ikeda et al.. teaches wherein content data is changed to a discrete instance ([0389] e.g. *Discrete instance, not defined, is interpreted as individually distinct*. http://www.merriam-webster.com/dictionary/discrete. As applied to Messerges, when locked content is to be moved, a "move" process is invoked such that deletion of contents of the copy source occurs. As applied to Messerges, copies of locked content are distributed to authorized devices. When a "move" operation is executed, such copies are required to be deleted. The result is a discrete instant or a single copy of the content. One of ordinary skill in the art would appreciate that when multiple copies, as per Messerges, are to be deleted, it is obvious to send a delete command to devices harboring the copied content. In support, Messerges teaches a domain authority, i.e., server, configured to send a delete command to a user device, i.e., sending a disable request ([0029] e.g.,

as applied to Ikeda et al., a delete request may readily be adapted to inform devices harboring copies to delete the copies when a "move" request is initiates, as per Ikeda et al.

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to modify Messerges to enable the bounded version (e.g, multiple copies are distributed and tied to a plurality of authorized, domain devices) to be moved outside the domain. Ikeda et al. teaches a "move" operation such that copies of the original content are deleted resulting in a single version. Messerges teaches a means to send delete commands to individual devices. Thus, when content is to be moved, as per Ikeda et al., it is obvious to delete copies from each of the devices harboring individual copies of the locked content data. As applied to Messerges, a single version of locked content may be moved from a first to a second domain while preserving ownership rights by deleting copies of a source (e.g. supra Messerges - 0036-37])

8. As per claim 2, Messerges et al. teaches the method of claim 1, wherein:
said locked content data and said license corresponding to said locked content data are stored on a the server device ([0042-49] e.g., requested content is provided from a content provider. The requested content, as part of the content package, further includes an electronic rights table, a rights document, encrypted content....The objects of the content package may optionally be provided by two files – a license file, encoded rights table, and an encrypted content, etc. As modified by Foster, such locked content would be stored on a participating device that functions as both a server and authorizer, supra Foster [COL [0080]))

9. As per claim 3, Messerges et al. teaches the method of claim 2, wherein:
presenting said locked content data includes decrypting said locked content data to produce

output content data and sending said output content data to said presentation component ([0060-62])

10. As per claim 5, Messerges et al. teaches he method of claim 1, wherein:

checking said license includes sending a confirm license request to said server from said client ([0060-61] e.g., a content package is opened via verifying the package's rights document, hash, and encoded rights table....As applied to Foster, a server| authorizer device includes the aforementioned function of checking a license prior to distributing content to the participating device)

11. As per claim 6, Messerges et al. teaches the method of claim 5, wherein:

presenting said locked content data includes receiving output content data streamed from said server device to said client ([0062] e.g., streaming content)

12. As per claim 7, Messerges et al. teaches the method of claim 5, further comprising:

checking a revocation list to determine whether said client is included in said revocation list ([0073], [0029], [0063-64], e.g., revocation list may be provided via a web server application);

wherein said revocation list indicates devices for which the license has been revoked, and wherein said revocation list is stored on said server device ([0073] e.g., this functionality may be provided via a web server. As applied, to Foster, a participating device functions as both server and authorizer. It is obvious to incorporate the functions of an external server, as per Messerges, into the device server|authorizer, as per Foster)

13. As per claim 8, Messerges et al. teaches the method of claim 1, further comprising:

checking a revocation list to determine whether said client is included in said revocation

list ([0029], [0063-64]);

wherein said revocation list indicates devices for which the license has been revoked, and wherein said revocation list is stored on said client ([0074], [Figure 11- element 1110])

14. As per claim 9, Messerges et al. teaches the method of claim 1, wherein: said locked content data is media data ([0031])

15. As per claim 10, Messerges et al. teaches he method of claim 1, wherein: said presentation component is integral to said client ([Figure 3- phones including a display)

16. As per claim 11, Messerges et al. teaches the method of claim 1, wherein: said presentation component is external to said client ([Figure 3- phones include an integrated, external display)

17. As per claim 12, Messerges et al. teaches the method of claim 1, wherein: said presentation component includes a television ([0003], [0040], [Figure 5- set-top box)

18. As per claim 13, Messerges et al. teaches the method of claim 1, wherein: said presentation component includes an audio speaker system ([0028], [Figure 5])

19. As per claim 14, Messerges et al. teaches a method of presenting content data, comprising:

receiving at a server connected to a hub network a present request indicating locked content data and indicating to a client connected to said hub network to present the content data ([0060-62]);

checking a license corresponding to said locked content data to determine if said license permits said server to present said locked content data through said client (([0060-61] e.g., verifying the package's rights document , hash, and encoded rights table),

wherein said locked content data is a bound instance if said license permits presentation of said locked content data by said server through said client connected to a-the hub network ([0060-63], [0037- 38], [0040], [Figure 4] e.g., all devices registered to a domain will be interconnected in that they will have access to content within the domain. Content is cryptographically bound to the domain ID), and

wherein the bound instance of said locked content data and the license corresponding to said locked content data are bound to the hub network ([0060-63], [0037-38], [0040], e.g., content is bound to the device domain); and

presenting said locked content data through a presentation component connected to said client when said locked content data is a bound instance ([0059-63], [Figure 3] e.g, before content may be played, the content manager invokes the core digital rights management software)

However, Messerges et al. does not teach the following limitations:

1] wherein the server device is configured to set up the hub network including adding the client and the server device to the hub network.
2] wherein the server device is configured to function as a client in the hub network, and
3] wherein said locked content data is stored on the server device connected to the hub network

Foster et al. teaches **1]** ([0080 lines 1-10] e.g., existing devices are both servers and authorizers. This is understood that participating devices function both as server and/or client.)

2] ([0080 line 9-11] e.g., sharing and distributing data)

3] ([0080] lines 9-11])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to modify Messerges as to enable participating devices to function as a server and client, control how many devices are added to the network, and control how content is

distributed within the network. The motivation is to implement the teachings of Foster et al. to localize content distribution opposed to requiring a client device to contact an external source for content, as per Messerges. Thus, it is obvious to make integral (e.g., adding, distributing, and authorizing content) content distribution with that of a local network).
authorizing content) content distribution with that of a local network).

However, Messerges et al., as modified, does not teach a) wherein said locked content data is changed to a discrete instance when said locked content data is to be moved to another server device bound to another hub network and b) the server device sends a disable request for the locked content data to clients of the hub network to indicate that the bound instance of the locked content data is changed to the discrete instance. Messerges et al. does teach the limitation of when said locked content data is to be moved to another server device bound to another hub network (see Fosters, [0079] e.g., obvious to relocate content to another domain. However, the copy will be disabled, see below, until rights are established via a source for that copy. As applied, a copy would be operable to be bound to another network by requesting such content to be bound, as per the teachings of Messerges, [0037] e.g., binding content to a particular domain);

Ikeda et al.. teaches wherein content data is changed to a discrete instance ([0389] e.g. *Discrete instance, not defined, is interpreted as individually distinct.* http://www.merriam-webster.com/dictionary/discrete. As applied to Messerges, when locked content is to be moved, a "move" process is invoked such that deletion of contents of the copy source occurs. As applied to Messerges, copies of locked content are distributed to authorized devices. When a "move" operation is executed, such copies are required to be deleted. The result is a discrete instant or a single copy of the content. One of ordinary skill in the art would appreciate that when multiple

copies, as per Messerges, are to be deleted, it is obvious to send a delete command to devices harboring the copied content. Messerges teaches a domain authority, i.e., server, configured to send a delete command to a user device, i.e., sending a disable request ([0029] e.g., as applied to Ikeda et al., a delete request may readily be adapted to inform devices harboring copies to delete the copies when a "move" request is initiates, as per Ikeda et al.

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to modify Messerges to enable the bounded version (e.g, multiple copies are distributed and tied to a plurality of authorized, domain devices) to be moved outside the domain. Ikeda et al. teaches a "move" operation such that copies of the original content are deleted resulting in a single version. Messerges teaches a means to send delete commands to individual devices. Thus, when content is to be moved, as per Ikeda et al., it is obvious to delete copies from each of the devices harboring individual copies of the locked content data. As applied to Messerges, a single version of locked content may be moved from a first to a second domain while preserving ownership rights by deleting copies of a source (e.g. supra Messerges - 0036-37])

20. As per claim 15, Messerges et al. teaches the method of claim 14, wherein: streaming data to said client includes streaming locked content data to said client ([0062])

21. As per claim 16, Messerges et al. teaches the method of claim 14, further comprising: decrypting said locked content data ([0060])

22. As per claim 17, Messerges et al. teaches the method of claim 14, wherein: said present request is received from said client ([0042], [0060])

23. As per claim 18, Messerges et al. teaches the method of claim 14, further comprising: checking a revocation list to determine whether said client is included in said revocation list ([0073], [0029], [0063-64], e.g., revocation list may be provided via a web server application);

wherein said revocation list indicates devices for which the license has been revoked, and wherein said revocation list is stored on said server ([0073] e.g., this functionality may be provided via a web server)

24. Claims 19-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Messerges et al. (USPN 20020157002 A1) in view over Russell et al. (20020069420), in view over Foster et al. (USPN 20030198351), and in further view over Ikeda et al. (USPN 20060098936)

25. As per claim 19, Messerges et al. teaches a method of copying content data, comprising:

receiving in a hub network a request indicating locked content data ([0031], [0045], [0053] e.g. users may wish to copy newly purchased content packages), ; and

copying said locked content data to produce a copy of said locked content data when said locked content data is a bound instance with a corresponding license that is bound to said hub network ([0062] e.g., streaming, copying, loaning, or moving content to other trusted devices);

wherein the bound instance if said locked content data and the license corresponding to said locked content data are bound to the hub network ([0062-64] e.g., trusted devices are interpreted as belonging to the authorized domain)

However, Messerges et al. does not teach a copy request and copying said locked content data to produce a copy of said locked content data. Messerges teaches said locked content data is a bound instance with a corresponding license that is bound to said hub network ([0062] e.g.,

streaming, copying, loaning, or moving content to other trusted devices). Messerges teaches a request for locked content data from a content provider ([0042]) Russell et al. teaches a main server containing copy of each content item ([0074], [0080])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to include a server copy of protected content for distribution. Since it is foreseeable that users would request a replacement of content that may have been corrupted, it would be necessary to provide a copy of the original content to the user opposed to sending the original content. Russell et al. illustrates that copies of content are maintained, and therefore it would have been obvious to enable the user to receive a copy of requested content.

However, Messerges et al. does not teach the following limitations:

1] wherein the server device is configured to set up the hub network including adding the client and the server device to the hub network.
2] wherein the server device is configured to function as a client in the hub network, and

Foster et al. teaches **1]** ([0080 lines 1-10] e.g., existing devices are both servers and authorizers. This is understood that participating devices function both as server and/or client.)

2] ([0080 line 9-11] e.g., sharing and distributing data)

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to modify Messerges as to enable participating devices to function as a server and client, control how many devices are added to the network, and control how content is distributed within the network. The motivation is to implement the teachings of Foster et al. to localize content distribution opposed to requiring a client device to contact an external source for

content, as per Messerges. Thus, it is obvious to make integral (e.g., adding, distributing, and authorizing content) content distribution with that of a local network).
authorizing content) content distribution with that of a local network).

However, Messerges et al., as modified, does not teach a) wherein said locked content data is changed to a discrete instance when said locked content data is to be moved to another server device bound to another hub network and b) the server device sends a disable request for the locked content data to clients of the hub network to indicate that the bound instance of the locked content data is changed to the discrete instance. Messerges et al. does teach the limitation of when said locked content data is to be moved to another server device bound to another hub network (see Fosters, [0079] e.g., obvious to relocate content to another domain. However, the copy will be disabled, see below, until rights are established via a source for that copy. As applied, a copy would be operable to be bound to another network by requesting such content to be bound, as per the teachings of Messerges, [0037] e.g., binding content to a particular domain);

Ikeda et al.. teaches wherein content data is changed to a discrete instance ([0389] e.g. *Discrete instance, not defined, is interpreted as individually distinct.* http://www.merriam-webster.com/dictionary/discrete. As applied to Messerges, when locked content is to be moved, a "move" process is invoked such that deletion of contents of the copy source occurs. As applied to Messerges, copies of locked content are distributed to authorized devices. When a "move" operation is executed, such copies are required to be deleted. The result is a discrete instant or a single copy of the content. One of ordinary skill in the art would appreciate that when multiple copies, as per Messerges, are to be deleted, it is obvious to send a delete command to devices harboring the copied content. Messerges teaches a domain authority, i.e., server, configured to

send a delete command to a user device, i.e., sending a disable request ([0029] e.g., as applied to Ikeda et al., a delete request may readily be adapted to inform devices harboring copies to delete the copies when a "move" request is initiates, as per Ikeda et al.

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to modify Messerges to enable the bounded version (e.g, multiple copies are distributed and tied to a plurality of authorized, domain devices) to be moved outside the domain. Ikeda et al. teaches a "move" operation such that copies of the original content are deleted resulting in a single version. Messerges teaches a means to send delete commands to individual devices. Thus, when content is to be moved, as per Ikeda et al., it is obvious to delete copies from each of the devices harboring individual copies of the locked content data. As applied to Messerges, a single version of locked content may be moved from a first to a second domain while preserving ownership rights by deleting copies of a source (e.g. supra Messerges - 0036-37])

26. As per claim 20, Messerges, as modified, teaches the method of claim 19, further comprising:

checking said license to determine if said license permits said locked content data to be copied ([0007] e.g., users request copies ,[0042], [0049] e.g., it is interpreted that in a digital rights management system that a user is verified prior to being provided digital content. As modified, a copy request would additionally include a verification of a user's permission)

27. As per claim 21 Russell et al, as modified, teaches the method of claim 19, further comprising:

requesting a new license from a server for said copy of said locked content data ([0037] e.g., new license); wherein said server is in said hub network and connected to said client (e.g., Messerges, as modified, teaches providing content to a network such that content is bound to the network. A server providing such content via the network is understood as being in a hub network)

28. As per claim 22, Messerges et al. teaches the method of claim 19, further comprising: sending said copy of said locked content data to a device that is not a member of said hub network ([0080] e.g., trusted devices outside the domain may be provided content if appropriate content protocol are supplied. As modified, it is interpreted that a content provider may provide copies to a device outside the authorized domain)

29. As per claim 23, Messerges et al. teaches the method of claim 19, further comprising: sending said copy of said locked content data to a client that is a member of said hub network but is not connected to said hub network ([0038], [0040] e.g., a device may receive data bound to a network but may not be physically connected to the network or within range of the domain yet still be a registered member of the domain. For example, a host PC may provide remote download to a device outside of the domain range, i.e., connectivity.)

Therefore, it would have been obvious to provide a host PC to provide content a device outside the immediate domain because such content will not be rendered until the device becomes part of or connected to the authorized domain.

30. As per claim 24, Russell et al. teaches sending a new license to a client that is a member of said hub network but is not connected to said hub network ([0037] e.g., it is interpreted that a new license may be associated with a portable device. [0038], [0040] e.g., a device may receive data bound to a network but may not be physically connected to the network or within range of

the domain yet still be a registered member of the domain. For example, a host PC may provide remote download to a device outside of the domain range, i.e., connectivity.)

Therefore, it would have been obvious to provide a host PC to provide content a device outside the immediate domain because such content will not be rendered until the device becomes part of or connected to the authorized domain.

31. As per claim 25, As per claim 8, Messerges et al. teaches the method of claim 1, further comprising:

checking a revocation list to determine whether said client is included in said revocation list ([0029], [0063-64]);

wherein said revocation list indicates devices for which the license has been revoked, and

wherein said revocation list is stored on said client ([0074], [Figure 11- element 1110])

32. As per claim 26, Messerges et al., as modified, teaches a method of distributing content data, comprising:

receiving from a providing device connected to a hub network, and at a receiving device a copy of locked content data that is a bound instance bound to said hub network ([Figure 1], [Figure 5], ([0042], [0049] e.g., requested content, i.e., receiving at a client, a request for locked content data, i.e., encrypted content file)

requesting a new license for said copy of locked content data (e.g., as modified in view of Russell, new license requests and receiving copies could be part of a user request for content. Please see Russell [0010], [0037], [0074]); and

receiving said new license for said copy of locked content data of the bound instance bound to said hub network (e.g., Messerges teaches binding content to a network, which as modified with

Russell, provides that copies of content and associated licenses are bound as well. Please see Messerges ([0060-63], [0037-38], [0040], e.g., content is bound to the device domain);

wherein the bound instance of said copy of locked content data and the new license corresponding to said copy of locked content data are bound to the hub network (e.g., Messerges teaches [0060-63], [0037-38], [0040], e.g., content is bound to the device domain);

However, Messerges et al. does not teach the following limitations:

1] wherein the providing device is configured to set up the hub network including adding the client and the providing device to the hub network.
2] wherein the providing device is configured to function as a client in the hub network, and
3] wherein said locked content data is stored on the providing device connected to the hub network

Foster et al. teaches **1]** ([0080 lines 1-10] e.g., existing devices are both servers and authorizers. This is understood that participating devices function both as server and/or client.)

2] ([0080 line 9-11] e.g., sharing and distributing data)

3] ([0080] lines 9-11])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to modify Messerges as to enable participating devices to function as a server and client, control how many devices are added to the network, and control how content is distributed within the network. The motivation is to implement the teachings of Foster et al. to localize content distribution opposed to requiring a client device to contact an external source for content, as per Messerges. Thus, it is obvious to make integral (e.g., adding, distributing, and authorizing content) content distribution with that of a local network).

authorizing content) content distribution with that of a local network).

However, Messerges et al., as modified, does not teach a) wherein said locked content data is changed to a discrete instance when said locked content data is to be moved to another server device bound to another hub network and b) the server device sends a disable request for the locked content data to clients of the hub network to indicate that the bound instance of the locked content data is changed to the discrete instance. Messerges et al. does teach the limitation of when said locked content data is to be moved to another server device bound to another hub network (see Fosters, [0079] e.g., obvious to relocate content to another domain. However, the copy will be disabled, see below, until rights are established via a source for that copy. As applied, a copy would be operable to be bound to another network by requesting such content to be bound, as per the teachings of Messerges, [0037] e.g., binding content to a particular domain);

Ikeda et al.. teaches wherein content data is changed to a discrete instance ([0389] e.g. *Discrete instance, not defined, is interpreted as individually distinct.* http://www.merriam-webster.com/dictionary/discrete. As applied to Messerges, when locked content is to be moved, a "move" process is invoked such that deletion of contents of the copy source occurs. As applied to Messerges, copies of locked content are distributed to authorized devices. When a "move" operation is executed, such copies are required to be deleted. The result is a discrete instant or a single copy of the content. One of ordinary skill in the art would appreciate that when multiple copies, as per Messerges, are to be deleted, it is obvious to send a delete command to devices harboring the copied content. Messerges teaches a domain authority, i.e., server, configured to send a delete command to a user device, i.e., sending a disable request ([0029] e.g., as applied to Ikeda et al., a delete request may readily be adapted to inform devices harboring copies to delete the copies when a "move" request is initiates, as per Ikeda et al.

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to modify Messerges to enable the bounded version (e.g, multiple copies are distributed and tied to a plurality of authorized, domain devices) to be moved outside the domain. Ikeda et al. teaches a "move" operation such that copies of the original content are deleted resulting in a single version. Messerges teaches a means to send delete commands to individual devices. Thus, when content is to be moved, as per Ikeda et al., it is obvious to delete copies from each of the devices harboring individual copies of the locked content data. As applied to Messerges, a single version of locked content may be moved from a first to a second domain while preserving ownership rights by deleting copies of a source (e.g. supra Messerges - 0036-37])

33. As per claim 27, Russell et al. teaches the method of claim 26, wherein: said providing device is a client in said hub network ([0107] e.g., user may copy and store the copy on another computer)

34. As per claim 28, Messerges et al. teaches the method of claim 26, wherein: said providing device is a server in said hub network ([Figure 2- element 210, 216 (e.g., computer acting as a server in view of Russell)

35. Claims 29-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Messerges et al. (USPN 20020157002 A1), in view over Foster et al. (USPN 20030198351), and in further view over Ikeda et al. (USPN 20060098936), in view over Russell et al. (20020069420), and in further view of Peinado et al. (USPN 20030217011)

36. As per claim 29, Messerges et al., as modified, does not teach said new license is received from said client. Peinado et al. teaches a license store may be embodied in any other form so long as the license store performs the function of storing licenses in a location convenient for the DRM [0132])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to utilize a client as a license store. As a member of an authorized domain, the client is authorized to access protected content. Since several authorized clients are also present within the network, it would have been obvious to use a client as a convenient means of providing a license to another client computer.

37. As per claim 30, Russell et al., as modified, teaches the method of claim 26 wherein said new license is provided from a server in said hub network ([Figure 2- element 12])

38. As per claim 31, Russell et al., as modified, teaches the method of claim 26 wherein said new license is received from an external server that is not in said hub network ([Figure 2 - element 16])

39. As per claim 32, Messerges et al., as modified, teaches the method of claim 26, wherein

said copy of locked content data has a corresponding license authority information stored on said providing device ([Figure 9], [0051], [0059], [0061], [0049] e.g., licensing authority, i.e., digital rights management software implements a content decoder to ask the content package manager to open a package. The content package is associated with a license)

said new license is received from a licensing authority indicated by said licensing authority information (e.g., Messerges et al., as modified by Russell et al, provides the ability to receive a

new license. The licensing authority information, i.e., package rights, provides access to such content)

40. As per claim 33, Messerges et al, as modified, teaches the method of claim 26, wherein said receiving device is not a member of said hub network ([0053], [0054] e.g., users may still request content from a provider via a user interface; however, such users outside the domain may not be able to access such content until such devices are registered with the domain)

41. As per claim 34, Messerges et al., as modified, teaches the method of claim 26, wherein said receiving device is a member of a second hub network ([Figure 4 – elements 202_1 202_2], [0040])

and said new license of said copy of locked content data is bound to said second hub network but not to said hub network ([Figure 4], [0040])

42. As per claim 35, Messerges et al. teaches the method of claim 26, wherein said receiving device is not connected to said hub network [0038], [0040] e.g., a device may receive data bound to a network but may not be physically connected to the network or within range of the domain yet still be a registered member of the domain. For example, a host PC may provide remote download to a device outside of the domain range, i.e., connectivity.)

Therefore, it would have been obvious to provide a host PC to provide content a device outside the immediate domain because such content will not be rendered until the device becomes part of or connected to the authorized domain.

43. As per claim 36, Messerges et al., as modified, teaches the method of claim 26, further comprising:

checking a revocation list to determine whether said receiving device is included in said revocation list ([0029], [0063-64]);

wherein said revocation list indicates devices for which the license has been revoked, and wherein said revocation list is stored on said receiving device ([0074], [Figure 11- element 1110])

44. As per claim 37, Messerges, as modified, teaches a method of distributing content data, comprising:

receiving at a server connected to a hub network, and from a device a request for a new license for a copy of locked content data that is a bound instance bound to said hub network (e.g., Messerges, as modified by Russell, teaches binding content to a network where a user may request a new copy of content. The copy of the content would be bound to the network. See Messerges [0042-44]. See Russell [0037- providing copies], supra claim 19 discussion);

checking a root license stored on said server to determine if said root license permits said server to provide a new license for said copy of locked content data of the bound instance ([0042], [0049] content provider, i.e., root server. As modified, a user requesting a new license would be verified as to whether they are permitted access to content. Furthermore, permitting a license to be provided, as taught by Russell, would include checking for payment, i.e., permitting a license to be issued ([0106]) ; and creating said new license according to said root license ([0031], [0042] , [0059], [0061] e.g., providing associated rights and permission. Messerges in view of Russell teaches that users may acquire a new license, where a set usage rules is established. A request for a new license would include usage rule); sending said new license to said device ([0037 (e.g., Russell) teaches downloading a license, i.e., receiving a license),

wherein said new license for said copy of locked content data of the bound instance is bound to said hub network ([0060-63], [0037- 38], [0040], [Figure 4] e.g., all devices registered to a domain will be interconnected in that they will have access to content within the domain. Content is cryptographically bound to the domain ID),

wherein the bound instance of said copy of locked content data and the new license are bound to the hub network ([0060-63], [0037-38], [0040], e.g., content is bound to the device domain. It is interpreted that content and associated license/usage rights are bound to the domain, in effect controlling who receives such content, i.e., registered with a domain, and how the content is rendered, i.e., set of usage rules - [0031])

However, Messerges et al. does not teach the following limitations:

1] wherein the providing device is configured to set up the hub network including adding the client and the providing device to the hub network.

2] wherein the providing device is configured to function as a client in the hub network, and

3] wherein said locked content data is stored on the providing device connected to the hub network

Foster et al. teaches **1]** ([0080 lines 1-10] e.g., existing devices are both servers and authorizers. This is understood that participating devices function both as server and/or client.)

2] ([0080 line 9-11] e.g., sharing and distributing data)

3] ([0080] lines 9-11])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to modify Messerges as to enable participating devices to function as a server and client, control how many devices are added to the network, and control how content is distributed within the network. The motivation is to implement the teachings of Foster et al. to localize content distribution opposed to requiring a client device to contact an external source for

content, as per Messerges. Thus, it is obvious to make integral (e.g., adding, distributing, and authorizing content) content distribution with that of a local network).

authorizing content) content distribution with that of a local network).

However, Messerges et al., as modified, does not teach a) wherein said locked content data is changed to a discrete instance when said locked content data is to be moved to another server device bound to another hub network and b) the server device sends a disable request for the locked content data to clients of the hub network to indicate that the bound instance of the locked content data is changed to the discrete instance. Messerges et al. does teach the limitation of when said locked content data is to be moved to another server device bound to another hub network (see Fosters, [0079] e.g., obvious to relocate content to another domain. However, the copy will be disabled, see below, until rights are established via a source for that copy. As applied, a copy would be operable to be bound to another network by requesting such content to be bound, as per the teachings of Messerges, [0037] e.g., binding content to a particular domain);

Ikeda et al.. teaches wherein content data is changed to a discrete instance ([0389] e.g. *Discrete instance, not defined, is interpreted as individually distinct.* http://www.merriam-webster.com/dictionary/discrete. As applied to Messerges, when locked content is to be moved, a "move" process is invoked such that deletion of contents of the copy source occurs. As applied to Messerges, copies of locked content are distributed to authorized devices. When a "move" operation is executed, such copies are required to be deleted. The result is a discrete instant or a single copy of the content. One of ordinary skill in the art would appreciate that when multiple copies, as per Messerges, are to be deleted, it is obvious to send a delete command to devices harboring the copied content. Messerges teaches a domain authority, i.e., server, configured to

send a delete command to a user device, i.e., sending a disable request ([0029] e.g., as applied to Ikeda et al., a delete request may readily be adapted to inform devices harboring copies to delete the copies when a "move" request is initiates, as per Ikeda et al.

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to modify Messerges to enable the bounded version (e.g, multiple copies are distributed and tied to a plurality of authorized, domain devices) to be moved outside the domain. Ikeda et al. teaches a "move" operation such that copies of the original content are deleted resulting in a single version. Messerges teaches a means to send delete commands to individual devices. Thus, when content is to be moved, as per Ikeda et al., it is obvious to delete copies from each of the devices harboring individual copies of the locked content data. As applied to Messerges, a single version of locked content may be moved from a first to a second domain while preserving ownership rights by deleting copies of a source (e.g. supra Messerges - 0036-37])

45. As per claim 38, Messerges, as modified, teaches the method of claim 37, where said device is not connected to said hub network ([0038], [0040] e.g., a device may receive data bound to a network but may not be physically connected to the network or within range of the domain yet still be a registered member of the domain. For example, a host PC may provide remote download to a device outside of the domain range, i.e., connectivity.)

Therefore, it would have been obvious to provide a host PC to provide content a device outside the immediate domain because such content will not be rendered until the device becomes part of or connected to the authorized domain.

39. As per claim 39, Messerges et al, as modified, teaches the method of claim 5, further comprising:

checking a revocation list to determine whether said client is included in said revocation list ([0073], [0029], [0063-64], e.g., revocation list may be provided via a web server application);

wherein said revocation list indicates devices for which the license has been revoked, and wherein said revocation list is stored on said server device ([0073] e.g., this functionality may be provided via a web server. As applied, to Foster, a participating device functions as both server and authorizer. It is obvious to incorporate the functions of an external server, as per Messerges, into the device server|authorizer, as per Foster)

Response to Amendment

40. The amendment, filed 11/20/2009, has been entered and made of record.

Response to Arguments

41. Applicant's arguments with respect to claims 1-3 and 5-39 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARRIN DUNN whose telephone number is (571)270-1645. The examiner can normally be reached on EST:M-R(8:00-5:00) 9/5/4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert DeCady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/DD/
11/28/10

Ramesh Patel
Primary Patent Examiner
Art Unit 2121

/Ramesh B. Patel/

Primary Examiner, Art Unit 2121